Introduction to Cryptography – Exercise no. 1

Submit in Pairs/Single to mailbox 19 by 23/3/11, 1:00 p.m.

The ciphertexts of questions 1, 2 are available as a text file in the courses homepage.

1. Decipher the following ciphertext, generated using substitution cipher:

```
XGZZO SFOOX KSKOL EXSKF OSJAE RETZS FJOWJ EXKZI OJIOF JISJX SJEGX GFSXU
XSJEG XWGAG XAOER OLSXL WGLOL EASJO LASXT GXKOX LQFOZ OSFOD OJGXS KFOSJ
HSJJT OMEOT LGMJI SJZSF ZOISR OAGDO JGLOL EASJO SCGFJ EGXGM JISJM EOTLS
WSMEX STFOW JEXKC TSAOM GFJIG WOZIG IOFOK SROJI OEFTE ROWJI SJJIS JXSJE
GXDEK IJTER OEJEW STJGK OJIOF MEJJE XKSXL CFGCO FJISJ ZOWIG QTLLG JIEW
```

   Explain the techniques you use, and describe all steps of your solution.

2. Decipher the following ciphertext, generated using Vigenére:

```
VUTZD LVAOJ MEWHK UTVUA ZOSEV OLCEI ZHKXI KKEXK EIHIT ZLVII KRHRW HUAWR
QDYCM WWCNG VZRTY GWDDN ENIRY YINEI LOZYE EGANA RUUEJ ZLFXS GTHDD IRIPR
GSURH ZHRYC MKKPX UZZVI UTWVQ OAMLK RCGXV PWHKS EKKOA YEEGL OZLVH XVKRU
LTAXI RWHUS IRQDG ZXYHF XURKL NIRYU LNMKR KHRZG MEPET ZSWJU KYXJV MGRPZ
WESYW LFHGY KCXEG THGDI TZEEG SASWJ SETZS EFHGX MFWSG THRUM UXAZO LXKET
KTNKX FWARU JRWHU AWRQD UARTH SULWZ OVKXT VUDGE
```

   Explain the techniques you use, and describe all steps of your solution.

3. Let $\mathcal{M}$, $\mathcal{C}$, and $\mathcal{K}$, be the plaintext, ciphertext, and key space, respectively. As usual, we assume that all elements are in the support of these spaces (i.e., have non-zero probability). Prove, or give a counterexample, for the following statements:

   (a) If a cipher is perfect with respect to some given plaintext distribution $\mathcal{P}$ then it is perfect for any plaintext distribution $\mathcal{P}'$.

   (b) If a cipher is perfect and $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$, then every ciphertext is equally probable.

   (c) If a cipher is perfect and $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$, then plaintext is equally probable.

   (d) If a cipher is perfect and $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$, then key is equally probable.

   (e) If $|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$, and all messages and keys are equally probable, then the cipher is perfect.

4. Prove that in DES, decryption is equivalent to encryption, up to the order of subkeys.

5. Devise a simple attack on three-round DES (the first three). The attack should use only one known plaintext/ciphertext pair, and its complexity must be bounded by 2^{30}. The attack may use the key schedule algorithm of DES. A bonus will be given to attacks whose time complexity is less than 2^{22}.

6. (a) Given an input and an output to DES F-function, how many different (48-bit) subkeys can lead from the given input to the given output?

   (b) Is it possible to find two subkeys K_1, K_2 and two inputs I_1 , I_2 for which $F(I_1, K_1) = F(I_2, K_2)$?
   If your answer is yes, provide such a set of values.

   (c) Is it possible to find a subkey K and two inputs I_1 , I_2 for which $F(I_1, K) = F(I_2, K)$?
   If your answer is yes, find such inputs for the subkey $K = 0F0F\ F0F0\ 0F0F_x$.